

REMARKS

The present amendment is submitted in response to the Non-Final Office Action mailed June 19, 2007. Claims 1-13 are currently pending in the application. No new matter or issues are believed to be introduced by this amendment. In view of the remarks to follow, reconsideration and allowance of this application are respectfully requested.

Objections to the Drawings

In the Office Action, the drawings were objected to for failing to comply with 37 CFR 1.21(d) because Figures 1 should be designated by a legend such as - - Prior Art - -. Applicants respectfully request withdrawal of the drawings objection and approval of the enclosed proposed drawing change.

Objection to the Specification

In the Office Action, the abstract of the disclosure was objected to because it does not commence on a separate sheet in accordance with 37 CFR 1.52 (b)(4). By means of the present a new Abstract is provided in a manner which is believed to overcome the objection. Withdrawal of the objection is respectfully requested.

Claim Rejections – 35 USC 101

In the Office Action, Claim 13 was rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claim 13 has been amended in a manner which is believed to overcome the rejection. Accordingly, withdrawal of the rejection is respectfully requested.

35 U.S.C. §102(b)

Claim 1-3 and 6-13 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Publication No. 2003/0091186 – Fontijn et al – hereinafter Fontijn.

It is respectfully submitted that independent claims 1-3 and 6-13 are patentable over Fontijn for at least the following reasons.

In the Office Action, the Examiner maintains, as per claim 1, that Fontijn teaches a record carrier (Figures 1, 4, block 4) for storing user data in sectors (par. 003) and management information associated with said sectors, (par. 0022, i.e., initialization vector stored in each header or sub-header of each block sector), wherein said management information comprises an encryption indication information indicating that the user data stored in the associated sector are to be encrypted by a read-out device before being transmitted over a communication bus (par. 0022, 22024, i.e., initialization vector can be used to contain encryption control information, re-encryption key data information is included in a read command).

It is respectfully submitted that Fontaijn does not teach the elements of claim 1, such as, *storing information on a record carrier to inform a read-out device regarding encryption information to be used to encrypt stored data before transmitting the data over a communication bus.*

The invention is directed to a low cost read out device that is optimized for the security level of a single application and a general purpose read out device that provides the right security level for all applications and can read record carriers for all applications. The invention provides a method for use by the general purpose read out device that can determine, if and, preferably, what type of encryption is to be used. Preferably, additional information is provided indicating if and which kind of decryption is required before encryption. Accordingly, Claim 1 recites a record carrier that stores user data in sectors and management information associated with each sector. The management information comprises encryption indication information (M1) indicating whether the user data stored in the associate sector is to be encrypted or not by a read-out device before being transmitted by a communication bus.

It is respectfully submitted that Fontaijn is not directed to providing a method for use by the general purpose read out device to determine, if and, preferably, what type of encryption is to be used on data retrieved from a stored medium, prior to sending the data over a communication bus, whereby the method comprises a record carrier that stores user data in sectors and management information associated with

each sector comprising encryption indication information (M1) indicating whether the user data stored in the associate sector is to be encrypted or not by a read-out device before being transmitted by a communication bus, as recited in claim 1.

Rather, Fontaijn is directed to solving a problem which arises whenever an apparatus receives a read or write command, e.g., from a PC application, and the apparatus cannot determine which key data to use to decrypt data already stored on the storage medium or which key data to use to encrypt data to be stored on the storage medium, since the apparatus does not receive the name of the file from the read or write command. Not receiving the file name makes it difficult, if not impossible, to determine the particular key data required to decrypt already encrypted data on the storage medium or to encrypt data to be stored on the storage medium.

Fontaijn overcomes this drawback by storing extra information together with the user data to allow the apparatus reading the user data to recognize if the user data is encrypted or not, and if so, which key data was used to encrypt the data. The extra information allows the apparatus to retrieve the correct key data *for decrypting* before outputting the data.

Fontaijn is also directed to *re-encrypting data* in the apparatus for reading after decrypting the user data read from the storage medium and before outputting the user data in re-encrypted form. In order to enable the apparatus for reading to re-encrypt the decrypted user data, a re-encryption key data information is included in a

read command (note: not stored on the storage medium as claimed by the invention) specifying which re-encryption key data to use for re-encryption. It is noted that, in contrast to the inventive method, which stores the encryption information on the storage medium for purposes of encrypting data before outputting the user data, Fontaijn includes the encryption information in a read command.

As described above, Fontaijn fully decouples the process of decryption and encryption. In Fontaijn, data stored on a storage medium is *decrypted* with the aid of extra information (an initialization vector) provided on the storage medium. It should be understood that Fontaijn stores extra information *only* for purposes of *decrypting already encrypted data*. The extra information informs the apparatus in two respects: (1) whether the user data stored on the storage medium is encrypted or not, and, (2) provides the correct key data to be retrieved for decrypting the data prior to outputting the data (in the case where the stored data is encrypted).

Fontaijn recites at Par. 39 -

[0039] When accessing the block or blocks on the medium 4 as indicated by the logical block address the reading means 5 do not only read the requested user data 21 but also, at first, an encryption indicator indicating if said user data 21 is encrypted or not. If said encryption indicator, which may be the first field of a header or sub-header of a block, indicates that the user data is encrypted a key data identifier specifying which key data to use for decrypting said user data is read from the header or sub-header of the same block. The key data itself can be stored in encrypted form on the storage medium, e.g. in a table of content (TOC) contained in a key locker, which can then be accessed by the reading means 5 using said key data identifier.

Fontaijn also teaches that once the data is decrypted, it may be *re-encrypted* prior to sending it over a communication bus. However, unlike the present invention which stores information on the storage medium for purposes of encrypting data to be sent over

a communication bus, the re-encryption process of Fontaijn utilizes encryption information provided in a *read command* provided by a *PC software application* to the read/write apparatus (See Fontaijn at par. 24). The key difference being that the encryption information for purposes of re-encrypting data to be transmitted over a communication bus is *not stored on the storage medium in Fontaijn*.

In the Office Action, the Examiner refers to Fontaijn at pars. 22 and 24, which recites – an initialization vector that can be used to contain encryption control information, re-encryption key data information is included in a read command. This refers to multiplexing the initialization vector (IV) with other information, e.g., information on partially encrypted blocks. In other words, the same bit string in the (sub-) header of a block on the disc may have two interpretations (at the same time). According to the first interpretation, it serves as an IV for decryption of the block. According to the second interpretation, it serves as encryption information for the data contained in the block. For example, in the second interpretation it may indicate that the stored data has been encrypted using algorithm E, where the encrypted portion of the block runs from position X and to position Y (i.e. the block is only partially encrypted). The advantage of this approach is that it saves some space in the (sub-) header of a block on the disc by not having to include two bit strings for the two purposes. This approach is made possible by the fact that the exact value of the IV is not relevant, as long as it is known by all parties that have to encrypt or decrypt the data contained in the block.

Accordingly, it is believed that Applicant's Claim 1 recites patentable subject matter, and therefore, withdrawal of the rejection with respect to Claim 1 and allowance thereof is respectfully requested.

Claims 2-3 and 6-7 depend from independent Claim 1 and therefore contain the limitations of Claim 1 and are believed to be in condition for allowance for at least the same reasons given for Claim 1 above. Accordingly, withdrawal of the rejection under 35 U.S.C. §102(b) and allowance of Claims 2-3 and 6-7 is respectfully requested.

Independent Claims 8-11 and 13 recite similar subject matter as Claim 1 and therefore contains the limitations of Claim 1. Hence, for at least the same reasons given for Claim 1, Claims 8-11 and 13 are believed to be allowable over Fontaijn. Accordingly, withdrawal of the rejection under 35 U.S.C. §102(b) and allowance of Claims 8-11 and 13 is respectfully requested.

Claim 12 depends from independent Claim 11 and therefore contain the limitations of Claim 11 and are believed to be in condition for allowance for at least the same reasons given for Claim 11 above. Accordingly, withdrawal of the rejection under 35 U.S.C. §102(b) and allowance of Claim 12 is respectfully requested.

35 U.S.C. §103(a)

In the Office Action, Claim 4 was rejected under 35 U.S.C. §103(a) as being unpatentable over Fontaijn in view of U.S. Patent No. 6,378,072 – Collins.

Claim 4 depends from Claim 1 and therefore includes the limitations of Claim

1. Accordingly, for the same reasons given above for Claim 1, Claim 4 is believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claim 4 is respectfully requested.

35 U.S.C. §103(a)

In the Office Action, Claim 5 was rejected under 35 U.S.C. §103(a) as being unpatentable over Fontaijn in view of U.S. Patent Application No. 2003/0159037 – Taki et al.

Claim 5 depends from Claim 1 and therefore includes the limitations of Claim

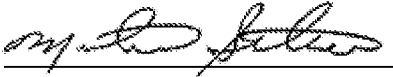
1. Accordingly, for the same reasons given above for Claim 1, Claim 5 is believed to contain patentable subject matter. Accordingly, withdrawal of the rejections with respect to Claim 5 is respectfully requested.

Conclusion

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims presently pending in the application, namely, Claims 1-13 are believed to be in condition for allowance and patentably distinguishable over the art of record.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Mike Belk, Esq. Intellectual Property Counsel, Philips Electronics North America, at 914-333-9643.

Respectfully submitted,



Michael A. Scaturro
Reg. No. 51,356
Attorney for Applicant

Mailing Address:
Intellectual Property Counsel
Philips Electronics North America Corp.
P.O. Box 3001
345 Scarborough Road
Briarcliff Manor, New York 10510-8001